A METHOD OF AND APPARATUS FOR GENERATION OF A KEY

FIELD OF THE INVENTION

The present invention relates to the field of data, device and communication protection and access control and in particular to a method of and apparatus for generation of a key.

BACKGROUND OF THE INVENTION

It is often necessary to protect data in digital form that is stored in data storage devices and/or transmitted over a network. To prevent un-authorized access of the data, encryption techniques are widely used. Essential problems of existing encryption techniques are (1) where to keep the encryption key, so that it remains safe and (2) how to authenticate a user in the most effective way. Currently, passwords and access cards or tokens are widely used for authentication. A password, however, can be easily attacked, and access cards can be easily lost. A user may lose valuable data forever if the password or card is forgotten or lost.

In order to address this problem, techniques have been proposed based on the use of biometrics of a user, that is to say, physical characteristics of the user that identify the user unambiguously. In several prior art proposals

such biometrics data is used to gain access to a computer system. The biometrics data is stored on a token for future reference. When the user subsequently wishes to obtain access to the system, the identity of the user is verified by comparing the biometrics data of the user with that stored on the token. These proposals have the disadvantage that a token is required, which may be lost or compromised. In U.S. 5613012, a tokenless identification system is disclosed based on a correlative comparison of a unique biometrics sample, such as a fingerprint or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.

These proposals have the disadvantage that an assumption is made that the storage devices are secure and that a secure communication link with the device is established. It is not true in many cases. In a networked environment, client devices can be public. Although the authorization data may be kept in a very secure place in the authenticating computer system, analogous to a safe deposit box in a bank, such data may still be accessible by the system operators and thus the data is not completely secure.

It is an object of the invention to provide a method of protecting digital data which alleviates this disadvantage of the prior art.

SUMMARY OF THE INVENTION

According to the invention, there is provided a method of generating a key or set of keys from a person's biometrics data comprising the steps of:

(1) capturing the person's biometric data;

(2) normalizing the captured biometrics data,

(3) extracting invariant feature measures from the normalized data and representing the feature measures as a bit pattern;

(4) storing the bit pattern in associative memory in an enrolment / registration phase and recalling the stored bit pattern from the associative memory in an identification / verification phase; and

(5) generating the key from the recalled bit pattern.

According to the invention in a second aspect, there is provided a method of generating a representation of biometrics data comprising the steps of:

(1) capturing the biometric data;

(2) normalizing the captured biometrics data,

(3) extracting invariant features from the normalized data and representing the features as a bit pattern.

According to the invention in a third aspect, there is provided a method of controlling access by generation of an access key from a person's biometrics data comprising the steps of:

(1) capturing the person's biometrics data;

(2) normalizing the captured biometrics data,

(3) extracting invariant features from the normalized data and representing the features as an initial bit pattern;

(4) storing the initial bit pattern in associative memory for retrieval;

(5) repeating steps (1)-(3) at a subsequent time to generate a subsequent bit pattern;

(6) inputting the subsequent bit pattern to the associative memory to recall the stored bit pattern; and

(7) generating the key from the recalled bit pattern.

According to the invention in a fourth aspect, there is provided a method of generating a key from the person's biometrics data which comprises the steps of:

(1) capturing the person's biometric data;

(2) normalizing the captured biometrics data,

(3) extracting invariant features from the normalized data and representing the features as a bit pattern;

(4) storing the bit pattern in associative memory for retrieval;and

(5) generating the key from the retrieved bit pattern.

The invention further comprises apparatus for performing any of the above methods.

According to the invention in a fifth aspect, there is provided a codebook to store data from which, upon

retrieval, a key is generated, the codebook comprising distributed associative memory.

The embodiment described is a tamper-resistant method and system to generate a unique key from biometrics of a person, using neural network associative memory. The captured biometrics data of a person may vary from time to time for reasons such as variation of the biometrics itself and variation of capturing conditions. The method compensates for this by first detecting invariant features from the biometrics. These features form feature measures in the format of a bit pattern which is stored in associative memory. At the authentication phase, the biometrics data is captured again from the user and the feature measures are again generated. The resulting bit pattern is then used to recall the bit pattern previously stored in the associative memory, which is unique to the user. A unique key can then be generated from the recalled pattern. Since associative memory is highly parallel and distributed, it is practically impossible to find exact patterns stored in the memory. Only a valid biometrics feature pattern can recall a valid stored pattern and generate a valid key for encryption and other purposes, such as for security, identity verification, as a PIN number or as a password.

The key may be of any kind, for example a public/private key pair, identity key or symmetry key.

BRIEF DESCRIPTION OF THE DRAWINGS

An embodiment of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a flow chart of the algorithm of an embodiment of the present invention.

Figure 2 illustrates the functions of parallel distributed associative memory in the embodiment of Figure 1.

Figure 3 illustrates feature points of a finger print.

Figure 4 illustrates a variation of the embodiment of the present invention in which multiple biometrics are combined for key generation.

Figure 5 illustrates another variation of the embodiment of the present invention using multiple associative memory codebooks.

DETAILED DESCRIPTION OF THE DESCRIBED EMBODIMENT

An embodiment of the method and apparatus to generate a unique private key for encryption / decryption, or a key for a digital lock, for secure communication, access control, ownership claiming and other applications will now

be described. In the following description, the overall flow chart of the system is first explained, followed by a detailed description of each step of the system. In this description, use of fingerprint and face (appearance) biometrics data will be used as examples, although it will be understood that the method is equally applicable for use with other biometrics data such as, but not limited to, hand geometry, hand vein, iris, retinal pattern, signature, voice print and facial thermograms. There will be differences in the initial step to convert the biometrics data into feature measures in the format of a bit pattern, but once the biometrics data has been converted into such feature measures, all other processing steps will be exactly the same for all types of biometrics.

As shown in Figure 1, the method has the following basic steps:

Biometrics data acquisition (1): In this step, acquisition devices such as a finger print scanner / sensor are used to capture image data or other forms of biometrics data.

Normalization of biometrics data (2): In this step, the data of Step 1 is processed in order to reduce the effect of variations due to capturing condition changes. Such processing includes scale change, translation, rotation, and lighting and background changes.

Feature encoding (3): In this step, feature measures which represent the invariant features of the biometrics are extracted and a bit pattern is generated from the feature measures.

Feature Registration and Matching (4): In this step the feature measure bit pattern is processed by a codebook 4a implemented as distributed associative memory. In an enrolment and registration step 4b, the bit pattern stored into the associative memory by learning. In a subsequent matching/recognition step 4c, a subsequently generated bit pattern is used to recall the bit pattern previously stored in the codebook to provide an activated pattern at step 4d.

Key Generation (5): In this step, a key is generated from the activated pattern. In case of enrolment/registration, the generated key is registered with the relevant authority or used to lock or encrypt the items to be protected. In case of matching/recognition, the
generated key is used to unlock or decrypt the items protected, or to authorize the person.

The techniques used in the each step will now be described:

1. Biometrics data acquisition

The technique employed for acquiring the biometrics data

depends on the biometrics used. In this description, fingerprint and face biometrics data are used as examples of the method. For fingerprints, either of the two primary techniques, i.e. inked or live scan may be used. With the inked method, an inked fingerprint image is taken and this is scanned into a computer. In the live scan technique, the fingerprint image is obtained by the scanner directly. For face, a digital picture of the face is obtained either through scanning of a photograph or directly with a digital camera. For both kinds of biometrics, biometrics data in the form of a digital image is obtained.

For additional authentication, it is desirable to capture live biometrics data, that is, the capture device must be able to verify that the biometrics data captured is from a live person. This can be done by by employing various techniques for various biometrics. For face recognition, where the video camera continuously captures a face image with a speed, for example of 30 frames per second, a processing function to check for motion of the face and facial expressions may be employed. If both face motion and facial expressions are regular, the face images captured are "live". They will be rejected as false otherwise. There are, similarly, scanners available which make use of the properties of a "live" fingerprint. In the case of speaker identification, the aquisition system can prompt the speaker to repeat a voice segment (eg a phrase or name) several times and check for variations, the

absence of which between any two segments will cause the biometrics data to be rejected.

2. Normalization of biometrics data

Normalisation in general is a common concept in image processing and is discussed, for example in A. Rosenfield, A. C. Kak, Digital image processing, Academic Press, New York, Second edition, 1982.

In the described embodiment, the biometrics data is normalised with reference to landmarks, which are central to the data and exist for all circumstances. The normalization is then done using these landmarks. By normalization is meant scaling the data range to a standard range and transforming the biometrics image to a standard location, orientation, and scale. The typical normalization methods for fingerprint and face biometrics data are well known in the art and examples are as follows:

Finger print: Filtering to enhance minutiae points, identification of the core (a small but consistent part of the finger) and use of the core location and orientation to define a geometric transform for normalization.

Face: Identify the face region and eyes, use the location of two eyes to define a geometric transform. Focus on face region and perform histogram normalization to reduce the

effect of background and lighting condition changes and transform the face image using the defined geometric transform.

3. Invariant feature extraction

In this step, a bit pattern is generated to represent the invariant features of the biometrics of a person. The bit pattern is not a binary version of the actual biometrics image but is formed by using salient feature points and possible lines linking those feature points. Figure 3 shows an example of feature points used to generate a bit pattern of a finger print. Here, salient feature points are highlighted with black points linked by the lines shown. Since invariant salient feature points are extracted from the normalized image, for the same person, the locations of those feature points would be almost the same. For fingerprint biometrics data, minutiae points of fingerprints are used as feature points. In the case of face biometrics, feature points such as the corners detected by Harris and Stephens (Harris, C. and Stephens, M. (1988) A combined corner and edge detector, Proc. 4th Alvey Vision Conference, pp 147-151) are invariant and can be used to form the bit pattern.

Feature points are of varying importance and a representation scheme for the bit pattern generation may be used. For example, in a fingerprint image, minutiae points

are considered more important than ridge points, so more (data) bits can be assigned to represent the minutiae points in the bit pattern.

The data forming the bit patterns may represent feature points from a smaller area than the original biometrics image with the central part emphasized, since parts far from central part may be missing in some cases.

4. Associative memory codebook and its operations

Associative memory codebooks can be implemented using various neural networks provided the stored patterns are randomly distributed. Hopfield-like networks are one of the possible implementations and will be used to explain this part of the described embodiment of the invention.

Supposing that the bit pattern extracted from the original biometrics image has size of M by N, then, there should be MN nodes in the Hopfield network. The network is fully connected. A node receives input from all other nodes. There is no distinction between input nodes, hidden nodes and output nodes. The total energy function of the network system is defined as summation of productions of value of all possible pairs of nodes and the link weight between them. The energy minima are referred to as stable states. The network stores information via its stable points in the

state space. The state evolution of the network system performs a gradient descent toward energy minima, and always ends up in a state of equilibrium. When the system reaches equilibrium, no state changes will happen to any node of the neural network system.

The bit patterns are stored by learning. One or several bit patterns representing the biometrics of a person are presented to the network as input and the network will evolve to create a stable state corresponding to the input patterns.

The information retrieval is performed by state evolution. When a subsequent input bit pattern is presented, all nodes obtain their initial state from the input bit pattern. The information is retrieved when the state evolution reaches a local stable point. The retrieved (activated) pattern is represented by states of MN nodes as a binary word of MN bits.

Figure 2 illustrates the functions provided by the associative memory which plays the roles of both matching/recognition (10) and biometrics database (12) of prior art methods. It is also coupled with the decision making (14) and key generation (16)/rejection (18) process in the sense that tolerance of distortion of the recalled bit pattern is reflected in the key generation, and that the key is directly generated from the recalled bit pattern

while in the prior art, the key is assigned using separated methods. By doing so, the method of the described embodiment successfully hides the biometrics database and the key generation methods, making them difficult to attack.

The key to be generated, which can be used as a public/private key pair and/or an identity key, requires more than 128 bits for security reasons. In the present method, the coordinates of salient points (around 48) are used to generate the private key, which can be as long as 48 x 2 bytes = 768 bits.

Using a Hopfield-like neural network as associative memory, for any given input pattern, the network evolution will converge to a stable state. The tamper resistance of the present method can best be explained in answer to the following question: if an attacker randomly input a biometrics pattern, what is the probability that the network converges to a stored valid biometrics pattern? This can be looked at in three ways:

1. Using the method of *steepest descent* or *Saddle-point approximation* (for example, as disclosed in the book "Neural Networks" by B. Muller J. Reinhardt, Springer-Verlag) it can be shown that in addition to the minima which correspond to the stored patterns, there are $\frac{1}{2}3^p$

spurious stable states for $p < N$, where p is the number of stored patterns. For a valid input pattern, there is no problem to converge to the corresponding minima since the starting point is very near the minima. But for a random input pattern, the probability of converging to a minima representing a valid biometrics patterns is very low: $2p3^{-p}$. Assume that there are 128 stored patterns, this probability will be much less than 2^{-128}, the attack probability for a 128 bit key. In the case of very few users, one can choose to store more (more than 128) patterns and only validate the few users.

2. When searching for a stored pattern with an input pattern by searching for minima of the energy function, the energy function actually represents the correlation between the input pattern and the stored pattern. As it is known that the correlation function usually does not have a sharp peak and noise exists, in practice, the recalled pattern is a mixture of the input pattern and the stored pattern (see book "Neural Networks and Simulation Methods" by Jian Kang WU, Marcel Dekker Inc.). The generated key will not be a valid one if the input pattern is quite different from the recalled one. That is to say, the input pattern must resemble the stored valid pattern in order to generate a valid key. By the nature of biometrics, there should not be any two identical biometrics patterns. That means that attacker must

randomly generate biometrics patterns which resemble the valid ones (at least, with certain degree of similarity). Assume that each pattern is characterized by 48 salient feature points and that the image size is 512 × 512, 18 bits are needed to code the coordinates of those points. To allow for 4 pixels variation of feature points, the 18 bits are reduced to 12 bits for coordinate coding. There are all together 48 × 12 = 576 bits to code a pattern. Since there are p valid stored patterns, the probability of resembling a valid pattern will be $p2^{-576}$

3. The storage capacity of Hopfield network can be as high as 2N even for non-orthogonal patterns using the learning method by Krauth and Mezard (See "Neural Networks" by B. Muller, J. Reinhardt; Springer-Verlag). To improve further the tamper-resistance of the system, a portion of the stored biometrics patterns can be validated. For a typical network size of 400 × 500, N=200,000. Within 400,000 stored patterns, only 400 patterns are validated. This further improves the tamper-resistance by reducing the attack probability by 1/1000.

5. Key Generation

In either the enrolment/registration (storage of bit pattern to associative memory) phase or the matching / recognition (pattern retrieval from associative memory)

phase, there is a stable state reached by network evolution. The states of nodes at the stable state represent the valid bit pattern of biometrics of a person. A unique key can be generated from the pattern.

Since there may be noise in the storage and retrieval process of the associative memory, it is preferred not to use directly the whole bit pattern represented by the network stable state to generate keys. Rather, only the most reliable and important feature points in the bit pattern are used. To decide on these points, a person to be enrolled in the enrolment/registration phase will repeat the step (1) of having his/her biometrics data captured as samples. The reliable feature points are defined as those points persistent for all sample biometrics data collected in the enrolment/registration phase.

When the important feature points are identified from the bit pattern, a hash algorithm (see book: Bruce Schneider, Applied Cryptography: protocols, algorithms and source code in C; John Wiley & Sons 1996) can be used to generate a unique key, that may be further used to generate the private key and public key for a specific application, such keys then being used to encrypt and decrypt data as this is input and output.

For some applications, the key needs to be changed within a certain period. This can be achieved by adding and

changing at least one parameter in the key generation program.

To achieve higher security, multiple biometrics can be combined for authentication. For example, using multiple finger prints, a combination of finger print with voice, etc. This is illustrated in Fig. 4 in which one set of processing modules 3-4d ...4d' ...4d" (capturing, normalisation, feature extraction and encoding, and registration/recall of associative memory codebook) for each biometrics is necessary to obtain recalled/activated pattern. All recalled/activated patterns (1, 2, ...,n) are then input to key generation module, and combined to generate one key.

In case of multiple data items of the same type of biometrics, for example, multiple finger prints, finger print data (1, 2, ...,n) are processed using one set of processing modules to obtain activated patterns for respective finger prints. When all recalled patterns arrive at the key generation module, a key is generated using all of recalled patterns.

If it is assumed that two finger prints are combined for authentication, since the false acceptance rate (FAR) for a finger print is 10^{-4}, combining two will result in FAR of 10^{-8}.

In case of large users, one associative memory may not be able to store all biometrics patterns. In such a case, multiple parallel associative memories 4a, 4a', 4a" and 4a'" can be used as illustrated in Fig. 5. Since such memories will run in parallel, the speed of authentication will not be reduced.

The method of the present invention can be implemented with a digital processor for example an ordinary computer, suitably programmed.